On Fermat's Last Theorem

C. Villacres— carlosvillacresjr@outlook.com

May 5, 2024

Abstract

Here we approach the problem of FLT using the Binomial Theorem and two cases: n even or odd. In this paper we will show that the polynomial $(a+b-c)^n$ can be factored iff $a^n+b^n=c^n$. Using this factored form we attain a general solution for FLT.

1 Fermat's Last and the Binomial Theorem

$a, b, c \in R^+$
and $n \geq 2 \in Z^+$

$$(a+b-c)^n = \sum_{j=0}^{n} \left(\begin{array}{c} n \\ j \end{array} \right) (-c)^j (a+b)^{n-j}$$

1.1 n, even

Suppose n is even, we get that

$$= c^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-c)^j (a+b)^{n-j} + (a+b)^n$$

Now we expand the last term,

$$(a+b)^n = a^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) a^j b^{n-j} + b^n$$

So,

$$(a+b-c)^n = c^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-c)^j (a+b)^{n-j} + a^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) a^j b^{n-j} + b^n,$$

$a^n + b^n = c^n \implies$

$$(a+b-c)^n = 2c^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-c)^j (a+b)^{n-j} + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) a^j b^{n-j}$$

$$= 2c^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) [(-c)^j (a+b)^{n-j} + a^j b^{n-j}] \tag{1}$$

If we can show that this polynomial is divisible by $(c-a)$, then it must also be divisible by $(c-b)$ since a and b are interchangeable. To do this, we will look at the same polynomial, but expanded differently.

$(a+b-c)^n = (-1)^n (c-a-b)^n = (c-a-b)^n \implies$

$$= b^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-b)^j (c-a)^{n-j} + a^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-a)^j (c)^{n-j} + c^n$$

$$= 2c^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) [(-b)^j (c-a)^{n-j} + (-a)^j c^{n-j}]$$

This shows that if $(c-a)$ is a factor of the polynomial, we only need to look at the second part of the sum along with the leading term to check.

We must show that

$$(c-a) \mid 2c^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-a)^j c^{n-j}.$$

If we plug in $c = a$ and get this equal to 0, then the original polynomial has a factor of $(c-a)$ (as well as $(c-b)$) for all n.

We get that $c = a \implies$

$$2a^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-a)^j a^{n-j} = 2a^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-1)^j a^j a^n a^{-j} = 2a^n + a^n \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-1)^j$$

If we look at Pascals Triangle, we can clearly see why this alternating sum would be $= -2$. Let's look at the 5th and 6th row of Pascals's Triangle as an example when $n = 6$.

For $n = 6$, the terms of the polynomial would be

$2a^6 + a^6(-6 + 15 - 20 + 15 - 6)$.

This can be rewritten with the 5th line of pascals coefficients:

$2a^6 + a^6(-(1+5) + (5+10) - (10+10) + (10+5) - (5+1))$.

So we can see that no matter what even n^{th} row we are in (without the 1's) we can use the $n-1^{th}$ row to rewrite the sum and show all middle coefficients cancel except the leading and last 1, so we get that

$\sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-1)^j = -2$ for all even n.

This $\implies 2a^n + a^n \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-1)^j = 0$ for all n, even.

This shows us that $(c-a)$ and $(c-b)$ are factors of the original equation. Finally, we get that for n, even:

$(a+b-c)^n = (c-a)(c-b)g_1(n)$ where

$$g_1(n) = \frac{2c^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) [(-c)^j(a+b)^{n-j} + a^j b^{n-j}]}{(c-a)(c-b)}.$$

We note here that $c-a$ and $c-b$ divide this polynomial just once each for any n. In other words, g_1 is not a rational equation and each term has an integer coefficient.

1.2 n, odd

For n odd, we do something similar. We get that

$$(a+b-c)^n = -c^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-c)^j(a+b)^{n-j} + a^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) a^j b^{n-j} + b^n$$

And $a^n + b^n = c^n \implies$

$$(a+b-c)^n = \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) [(-c)^j(a+b)^{n-j} + a^j b^{n-j}]$$

$$= (a+b)\sum_{j=1}^{n-1}\left(\begin{array}{c} n \\ j \end{array}\right)[(-c)^j(a+b)^{n-j-1} + \frac{a^jb^{n-j}}{(a+b)}] \tag{2}$$

We can show that $(a+b) \mid \sum_{j=1}^{n-1}\left(\begin{array}{c} n \\ j \end{array}\right) a^jb^{n-j}$ by plugging in a=-b. If the result is zero, then (a+b) is a factor.

$\sum_{j=1}^{n-1}\left(\begin{array}{c} n \\ j \end{array}\right)(-b)^jb^{n-j} = b^n\sum_{j=1}^{n-1}\left(\begin{array}{c} n \\ j \end{array}\right)(-1)^j = b^n0 = 0$

This is, again, because the odd rows of Pascal's Triangle would cancel each other out as each term would have its negative in the same row.

Let's define $g(n)$ s.t.

$$g(n) = \begin{cases} (c-a)(c-b)g_1(n), & \text{if } n \text{ is even} \\ (a+b)g_2(n), & \text{if } n \text{ is odd .} \end{cases}$$

Where $g_1(n) =$

$$\frac{2c^n + \sum_{j=1}^{n-1}\left(\begin{array}{c} n \\ j \end{array}\right)[(-c)^j(a+b)^{n-j} + a^jb^{n-j}]}{(c-a)(c-b)},$$

and $g_2(n) =$

$$\sum_{j=1}^{n-1}\left(\begin{array}{c} n \\ j \end{array}\right)[(-c)^j(a+b)^{n-j-1} + \frac{a^jb^{n-j}}{(a+b)}].$$

1.3 Fermat's Last Theorem, proof

We have that $(a+b-c)^n = (c-a)(c-b)g_1(n)$ for n, even. And $(a+b-c)^n = (a+b)g_2(n)$ for n, odd.

N, Even

This means that if a, b, c are integers, then $k = a+b-c = [(c-a)(c-b)g_1(n)]^{1/n}$, $\Longrightarrow$ that k has to be a multiple of the integer $g_1(n)$. So we get that,

$$k = g_1(n)\left(\frac{(c-a)(c-b)}{g_1(n)^{n-1}}\right)^{1/n}.$$

We'll show this only works for $n = 2$, where $g_1(2) = 2$.

$$k = 2\sqrt{\frac{(c-a)(c-b)}{2}}$$

We can let

$a = (c - b) + g(2)^{1/2}$,
$b = (c - a) + g(2)^{1/2}$,
$c = (a + b) - g(2)^{1/2}$

and define r,s such that

$r = (c - a)^{1/2}, s = [2(c - b)]^{1/2}$.

So we get

$a = s^2/2 + rs$

$b = r^2 + rs$

$c = s^2/2 + r^2 + rs$

Finally we get $k = 2\sqrt{\frac{(c-a)(c-b)}{2}} = 2(rs/2) = rs$ with the condition that rs is an even integer.

For $n = 4$ we get that $g_1(4) = 2(c - a)(c - b) + 4(a^2 + ab + b^2) \implies$

$$k = g_1(4)\sqrt[4]{\frac{(c-a)(c-b)}{[2(c-a)(c-b) + 4(a^2 + ab + b^2)]^3}}.$$

Upon close inspection, that radical will always be less than 1. This means that for $n \geq 4$, a+b-c is not a factor of the integer $g_1(n)$. So we get a contradiction that a,b,c were all integers.

N, Odd

For $n = 3$ we get that $g(3) = 3(a + b)(c - a)(c - b)$

$a = (c - b) + g(3)^{1/3}$, $b = (c - a) + g(3)^{1/3}$, and $c = (a + b) - g(3)^{1/3}$.

We will define r, s, t so that $r = (c-a)^{1/3}, s = (c-b)^{1/3}$, and $t = g(3)^{1/3}/rs = [3(a+b)]^{1/3}$. This means that we get

$(a+b-c)^3 = 3(a+b)(c-a)(c-b)$ or

$(rst)^3 = 3(r^3+s^3+2rst)(r^3)(s^3) \implies$

$t^3 = 3(r^3+s^3+2rst) \implies$ the cubic

$t^3 - 6rst - 3(r^3+s^3) = 0.$

Let p be a factor of r or s WLOG. Using Eisenstein's criterion with that prime number, we can see this cubic is irreducible. t has no integer solutions.

This cubic is interesting because of its form similar with the family of elliptic curves $y^2 = x^3 + ax + b$. In any case, the way we show n=5 also applies for n=3, but the elliptic equation seemed worth noting.

For $n = 5, g_2(5) = 5(c-a)^2(c-b)^2 + 5(a^2+b^2)(c-a)(c-b)$ which would imply that

$$k = a+b-c = g_2(5)\sqrt[5]{\frac{a+b}{[5(c-a)^2(c-b)^2+5(a^2+b^2)(c-a)(c-b)]^4}}$$

Again, we can see that the radical is less than 1, so since $g_2(5)$ is not a multiple of a+b-c, then a+b-c can't be integers. This applies for $n \geq 3$.

End proof.

Note: We could also show that for n odd, g(n) is also factorable by (c-a)(c-b) for all n odd (and thus all n). This would generalize the proof further. However, for n odd, given that it was divisible by (a+b) was easier to show and enough.

2 n=2

$$(a+b-c)^2 = g(2) = 2(c-a)(c-b) \tag{3}$$

Because of the relevance of right triangles, we get trigonometry.

$a = k(cos\theta),$ $\quad b = k(sin\theta),$ $\quad c = k$

$\implies$

$(cos\theta + sin\theta - 1)^2 = 2(1 - cos\theta)(1 - sin\theta)$

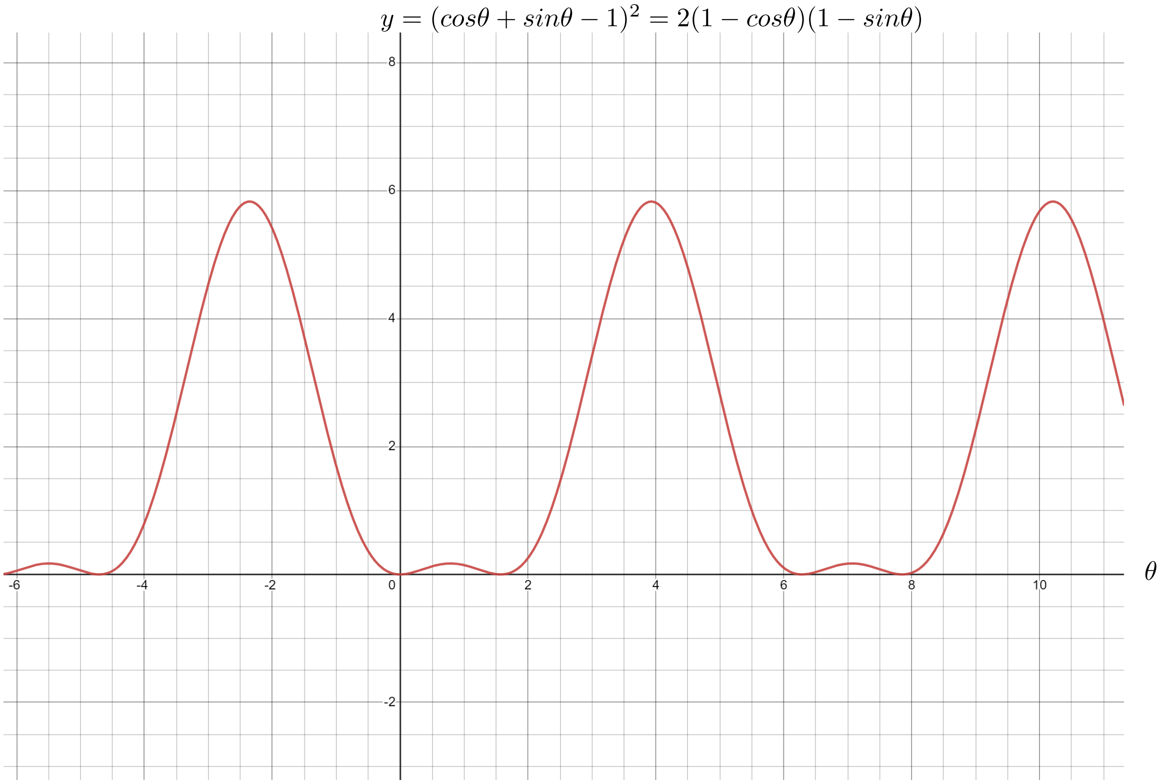
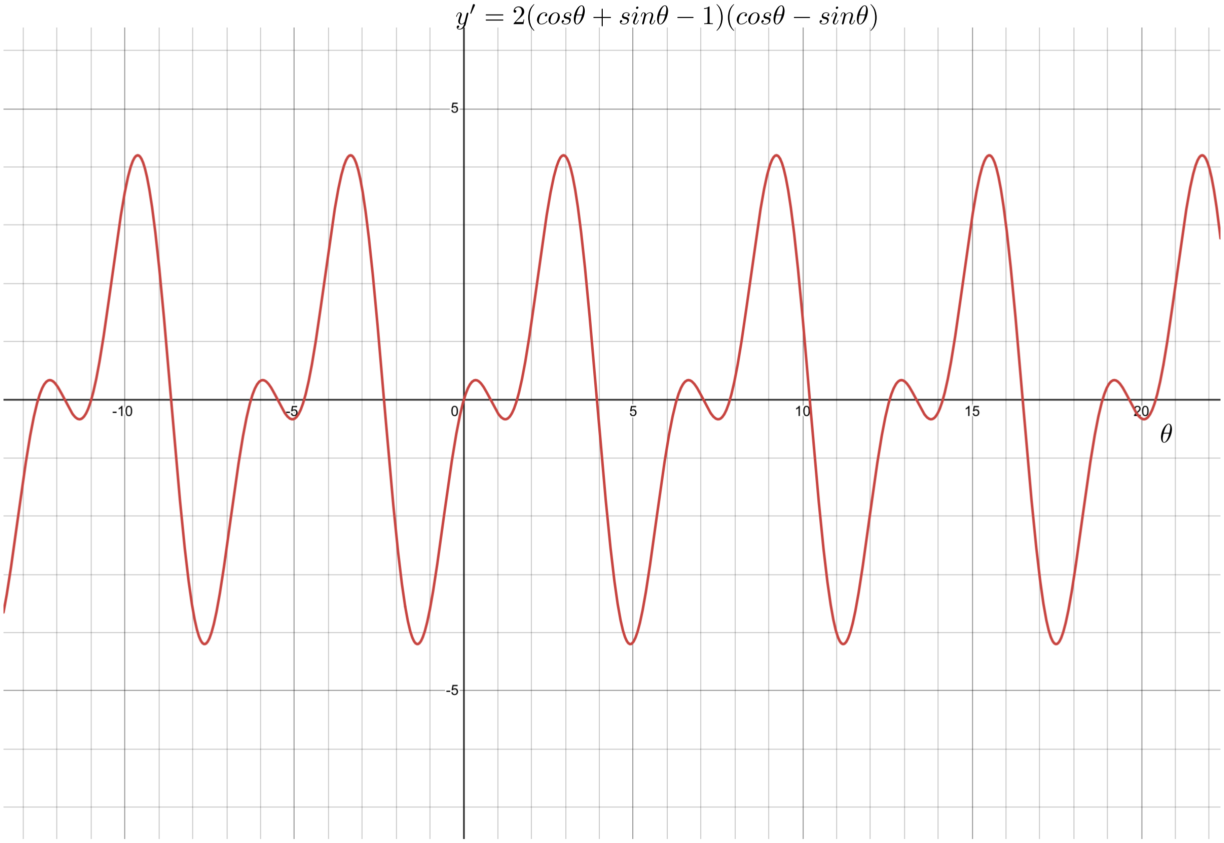

$y = (cos\theta + sin\theta - 1)^2 = 2(1 - cos\theta)(1 - sin\theta)$

Figure 1: This shows the identity as a function of theta. Notice the identity is ≥ 0. It also has an interesting rhythm to it.



$$y' = 2(cos\theta + sin\theta - 1)(cos\theta - sin\theta)$$

Figure 2: The derivative resembles the rhythm of a heartbeat.

2.1 General form of the n^{th} derivative of the trig identity

Here we will simply look at the form of the n^{th} derivative since it has a consistent form.
$y = (cos\theta + sin\theta - 1)^2$

Let $y^{(n)}$ represent the n^{th} derivative. Then,

$$y^{(n)} = \begin{cases} 2(cos\theta + sin\theta - 2^n sin\theta cos\theta)(-1)^{\frac{n}{2}-1}, & \text{if } n \text{ is even} \\ (2^n(cos\theta + sin\theta) - 2)(cos\theta - sin\theta)(-1)^{\frac{n-1}{2}}, & \text{if } n \text{ is odd .} \end{cases}$$

When we investigate the zeroes of the derivative forms, we obtain some interesting trig problem:

For n, even, setting $y^{(n)} = 0$ gives us that

$cos\theta + sin\theta = 2^n cos\theta sin\theta.$

Solving this using trig substitutions to change everything in terms of $sin(\theta+\pi/4)$ gives us a general solution for the zeros.

$\theta = sin^{-1}[2^{-(n+\frac{1}{2})} \pm (2^{-1} + 2^{-1-2n})^{\frac{1}{2}}] - \pi/4 + 2\pi k$ and

$\theta = 3\pi/4 - sin^{-1}[2^{-(n+\frac{1}{2})} \pm (2^{-1} + 2^{-1-2n})^{\frac{1}{2}}] + 2\pi k$ for any integer, k.

For n, odd we get an easier trig problem finding the zeros of

$cos\theta + sin\theta = 2^{1-n}$ and $cos\theta = sin\theta$.

2.2 Pythagorean Triples and $\sqrt{2}$

$(a + b - c)^2 = g(2) = 2(c - a)(c - b) \implies$

We have the Pythagorean Triple generator where s is any even integer, r any integer using the substitution from before:

$a = \frac{s^2}{2} + rs$

$b = r^2 + rs$

$c = \frac{s^2}{2} + r^2 + rs$

Note: It's actually only necessary that rs is an integer. For example $r = s = \sqrt{2}$. A special case if $r = s$:

This gives us,

$a = 3\frac{s^2}{2}$

$b = 4\frac{s^2}{2}$

$c = 5\frac{s^2}{2}$

Which is the famous 3,4,5 triple and its multiples.
We can see this when we let $s = \sqrt{2k_1}$ where $k_1 = (c - b)$.

Finally, we also get a form of $\sqrt{2}$ and a form of $\sqrt[3]{3}$.

$$\sqrt{2} = \frac{a+b-c}{\sqrt{(c-a)(c-b)}} \text{ iff } a^2 + b^2 = c^2$$
$$\sqrt[3]{3} = \frac{(a+b-c)}{\sqrt[3]{(a+b)(c-a)(c-b)}} \text{ iff } a^3 + b^3 = c^3$$

Which could also be written in an infinite power form since $2 = \frac{(a+b-c)^2}{(c-a)(c-b)}$ and $2^{-1} = \frac{(c-a)(c-b)}{(a+b-c)^2}$

Let $A = a + b - c$ and $B = (c - a)(c - b)$

$\sqrt{2} = \frac{A}{B^{2^{-1}}} = \frac{A}{B^{\frac{B}{A^2}}} = ...$

3 g(n) and the K-Form

We will end this with a general form of g(n).

We will let $k = (c - a)(c - b)$. Then, we can re-express $g(n)$ as a summation in terms of k. First we will look at the case where n is even and then when n is odd. The motivation behind this form is to focus on the reconstruction of the Binomial Coefficients for the n'th row we are in. If for $k^j = [(c-a)(c-b)]^j$ we focus on the constant term '$(ab)^j$', then it comes clear our choice for f_j.

When n is even,

$$g(n) = \sum_{j=1}^{n/2} f_j k^j$$

$f_{n/2} = 2$

$$f_j = \eta_j \sum_{\xi=0}^{n-2j} a^{\xi} b^{n-2j-\xi} \quad \text{where} \quad \eta_j = \begin{cases} \begin{pmatrix} n \\ j \end{pmatrix}, & \text{if } j = 1 \\ \begin{pmatrix} n \\ j \end{pmatrix} - \begin{pmatrix} n \\ j-1 \end{pmatrix}, & \text{else.} \end{cases}$$

And lastly, we will show that for $n \geq 6$ we will also need

$$f_{n/2-1} = [T_1 T_2 T_3] \cdot \begin{bmatrix} a^2 \\ ab \\ b^2 \end{bmatrix}$$

Where $T_1 = T_3 = \begin{pmatrix} n \\ \frac{n}{2} - 1 \end{pmatrix} - \begin{pmatrix} n \\ \frac{n}{2} - 2 \end{pmatrix}$ and $T_2 = \begin{pmatrix} n \\ \frac{n}{2} \end{pmatrix} - \begin{pmatrix} n \\ \frac{n}{2} - 2 \end{pmatrix} - 2$.

For convenience, we can also express k^j in its convoluted form. Namely,

$k^j = (a_j * b_j) \cdot c_{2j}$

where $a_j = \left[\begin{pmatrix} j \\ k_1 \end{pmatrix} (-a)^{k_1} \right]$, and $b_j = \left[\begin{pmatrix} j \\ k_1 \end{pmatrix} (-b)^{j-k_1} \right]$ for $k_1 = 0, 1, ...j$

$c_{2j} = \left[c^{k_2} \right]$ for $k_2 = 0, 1, ..., 2j$.

Let's do some examples. For n=2:

$g(2) = f_1 k^1$ where $f_1 = 2$ so,

$g(2) = 2k = 2(c-a)(c-b)$.

For n=4:

$g(4) = f_2 k^2 + f_1 k^1$ where $f_2 = 2$ and $f_1 = \eta_1 \sum_{\xi=0}^{2} a^{\xi} b^{2-\xi} = 4(a^2 + ab + b^2)$.

$g(4) = 2k^2 + 4(a^2 + ab + b^2)k$

For n=6 (and on) we start using the "trident" $[T_1 T_2 T_3]$.

$g(6) = f_3 k^3 + f_2 k^2 + f_1 k^1$

$f_3 = 2$ and $f_2 = [T_1 T_2 T_3] \cdot \begin{bmatrix} a^2 \\ ab \\ b^2 \end{bmatrix}$ where $T_1 = T_3 = 9, T_2 = 12$

and $f_1 = \eta_1 \sum_{\xi=0}^{4} a^{\xi} b^{4-\xi} = 6(a^4 + a^3 b + a^2 b^2 + ab^3 + b^4)$

So, $g(6) = 2k^3 + (9a^2 + 12ab + 9b^2)k^2 + 6(a^4 + a^3 b + a^2 b^2 + ab^3 + b^4)k$

Let's do one more, n=8:

$g(8) = f_4 k^4 + f_3 k^3 + f_2 k^2 + f_1 k^1$.

$f_4 = 2$, $f_3 = [T_1 T_2 T_3] \cdot \begin{bmatrix} a^2 \\ ab \\ b^2 \end{bmatrix}$ where $T_1 = T_3 = 56 - 28 = 28, T_2 = 70 - 28 - 2 = 40$

$f_2 = \eta_2 \sum_{\xi=0}^{4} a^{\xi} b^{4-\xi}$ where $\eta_2 = 28 - 8 = 20$.

So we get $f_2 = 20(a^4 + a^3 b + a^2 b^2 + ab^3 + b^4)$.

$f_1 = \eta_1 \sum_{\xi=0}^{6} a^{\xi} b^{6-\xi}$ and $\eta_1 = 8$.

Finally, we get that $g(8) =$

$2k^4 + (28a^2 + 40ab + 28b^2)k^3 + 20(a^4 + a^3 b + a^2 b^2 + ab^3 + b^4)k^2 + 8(a^6 + a^5 b + a^4 b^2 + a^3 b^3 + a^2 b^4 + ab^5 + b^6)k$.

When n is odd,

$$\frac{g(n)}{a+b} = \sum_{j=1}^{(n-1)/2} f_j k^j$$

$$f_{(n-1)/2} = n$$

$$f_j = \eta_j \sum_{\xi=0}^{(n-1-2j)/2} [a^{\xi} b^{(n-1-2j)/2-\xi}]^2 \quad \text{where } \eta_j = \begin{cases} \begin{pmatrix} n \\ j \end{pmatrix}, & \text{if } j = 1 \\ \begin{pmatrix} n \\ j \end{pmatrix} - \begin{pmatrix} n \\ j-1 \end{pmatrix}, & \text{else.} \end{cases}$$

And lastly, we will show that for $n \geq 7$ we will also need

$$f_{(n-3)/2} = [T_1 T_2 T_3] \cdot \begin{bmatrix} a^2 \\ ab \\ b^2 \end{bmatrix}$$

Where $T_1 = T_3 = \begin{pmatrix} n \\ \frac{n-3}{2} \end{pmatrix} - \begin{pmatrix} n \\ \frac{n-5}{2} \end{pmatrix}$ and $T_2 = \begin{pmatrix} n \\ \frac{n-1}{2} \end{pmatrix} - \begin{pmatrix} n \\ \frac{n-3}{2} \end{pmatrix} - n$.

And some examples for n, odd. When n=3:

$\frac{g(3)}{a+b} = f_1 k^1$ where $f_1 = 3$ so we get

$\frac{g(3)}{a+b} = 3k$

For n=5:

$\frac{g(5)}{a+b} = f_2 k^2 + f_1 k^1$ where $f_2 = 5$ and

$f_1 = \eta_1 \sum_{\xi=0}^{1} [a^\xi b^{1-\xi}]^2 = 5(a^2 + b^2)$ so we get that

$\frac{g(5)}{a+b} = 5k^2 + 5(a^2 + b^2)k$

For n=7 we start using the 'trident' like before:

$\frac{g(7)}{a+b} = f_3 k^3 + f_2 k^2 + f_1 k^1$ where $f_3 = 7$ and

$f_2 = [T_1 T_2 T_3] \cdot \begin{bmatrix} a^2 \\ ab \\ b^2 \end{bmatrix}$ where

$T_1 = T_3 = 21 - 7 = 14$ and $T_2 = 35 - 21 - 7 = 7$, and lastly,

$f_1 = \eta_1 \sum_{\xi=0}^{2} [a^\xi b^{2-\xi}]^2 = 7(a^4 + a^2 b^2 + b^4)$. So,

$\frac{g(7)}{a+b} = 7k^3 + (14a^2 + 7ab + 14b^2)k^2 + 7(a^4 + a^2 b^2 + b^4)k$.

Let's do n=9:

$\frac{g(9)}{a+b} = f_4 k^4 + f_3 k^3 + f_2 k^2 + f_1 k^1$ where $f_4 = 9$ and

$f_3 = [T_1 T_2 T_3] \cdot \begin{bmatrix} a^2 \\ ab \\ b^2 \end{bmatrix}$ where $T_1 = T_3 = 84 - 36 = 48$ and $T_2 = 126 - 84 - 9 = 33$

$f_2 = \eta_2 \sum_{\xi=0}^{2} [a^{\xi} b^{2-\xi}]^2 = (36 - 9)(a^4 + a^2b^2 + b^4)$

$f_1 = \eta_1 \sum_{\xi=0}^{3} [a^{\xi} b^{3-\xi}]^2 = 9(a^6 + a^4b^2 + a^2b^4 + b^6)$. So we get that g(9) is:

$\frac{g(9)}{a+b} = 9k^4 + (48a^2 + 33ab + 48b^2)k^3 + 27(a^4 + a^2b^2 + b^4)k^2 + 9(a^6 + a^4b^2 + a^2b^4 + b^6)k$

References

None

2020 Mathematics Subject Classification: 11D41